David J. Jordan (#1751)
Email: djordan@foley.com
David L. Mortensen (#8242)
Email: dmortensen@foley.com
Tyler A. Dever (#15584)
Email: tdever@foley.com
FOLEY & LARDNER LLP
95 S. State Street, Suite 2500
Salt Lake City, UT 84111
Telephone: 801.401.8900

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT FOR

THE DISTRICT OF UTAH

ALEGEUS TECHNOLOGIES, LLC, a Delaware limited liability company, Plaintiff, v. DIGICERT, INC., a Utah corporation, Defendant.	**EX PARTE MOTION FOR TEMPORARY RESTRATING ORDER AND PRELIMINARY INJUCTION** Civil No. 2:24-cv-00534-HCN The Honorable Howard C. Nielson, Jr.

Pursuant to Rule 65 of the Federal Rules of Civil Procedure, plaintiff Alegeus Technologies, LLC ("Alegeus"), by and through its counsel, respectfully moves this Court to enter a temporary restraining order and preliminary injunction precluding DigiCert, Inc. ("DigiCert") from decertifying or revoking certain digital security certificates relating to Alegeus' vendor websites a period of seven (7) days.

INTRODUCTION AND RELIEF REQUESTED

Because of an error committed by DigiCert, yesterday at around 4:40 p.m., DigiCert informed Alegeus that it had until 1:30 p.m. today (e.g. less than 21 hours) to reissue and reinstall the security certificates (collectively, the "Security Certificates") for 72 of its websites (collectively, the "Alegeus Websites"). DigiCert stated that if Alegeus failed to do so, it would revoke the security certificates for those websites. Alegeus immediately began trying to reissue and reinstall the Security Certificates but it simply cannot complete that entire process for all 72 websites in 21 hours for reasons further explained below. Accordingly, Alegeus requested three days to rekey and reissue the Security Certificates. DigiCert refused. If DigiCert decertifies or revokes the Security Certificates, it will cause Alegeus, its clients and their millions of health plan participants severe and irreparable harm. Accordingly, Alegeus seeks an immediate and expedited TRO to prevent DigiCert from decertifying or revoking the Security Certificates for the Alegeus Websites.

As set forth in greater detail below, Alegeus is a leading provider of a business-to-business, white-label funding and payment platform for healthcare carriers and third-party administrators to administer consumer-directed employee benefit programs, including HSAs, FSAs, HRAs, COBRA, health and wellness programs, dependent care accounts and transportation accounts serving millions of U.S households (collectively, the "Health Accounts"). Specifically, Alegeus is designated as a non-bank health savings trustee ("NBT") by the United States Internal Revenue Services (the "IRS"). This designation allows it to serve as the custodian of Health Savings Accounts ("HSAs") through a direct custodial agreement with the HSA accountholders.

As part of its business, Alegeus contracts primarily with health plans and third-party administrators (the "Alegeus Clients" or "Clients") who manage these Health Accounts to provide a platform where individuals with Health Accounts can manage their accounts by, among other things, paying health providers for medical services, submitting claims for reimbursement, checking account balances, and making contributions. Alegeus provides unique websites and domain names for the Alegeus Clients—those websites are the Alegeus Websites. Alegeus Clients contract with employers to provide the employers with the services related to the Health Accounts and the employers make available the benefits of the Health Accounts to their employees. These employees are typically referred to as plan participants. Alegeus does not contract directly with employers.

1. To ensure the Alegeus Websites have the necessary Security Certificates, Alegeus entered into a Master Services Agreement and related agreements (collectively, the "Master Service Agreement") with DigiCert to provide digital security certificates for the Alegeus Websites. *See* Master Services Agreement, Compl. at Ex. 1. Specifically, DigiCert provides public key infrastructure ("PKI") and validation required for issuing digital certificates or TLS/SSL certificates (collectively, the "Security Certificates") for the Alegeus Websites. About thirty days ago, Alegeus worked with DigiCert to update many of the Security Certificates for the Alegeus Websites. Alegeus followed DigiCert's instructions for updating the Security Certificates.

Following such updates, and without any interim notification of any issues, yesterday at 4:40 p.m., DigiCert sent an email to Alegeus stating that "DigiCert would be revoking [the Security Certificates]" unless Alegeus reissued/rekeyed and reinstalled the impacted certificates by 7:30 p.m. (Coordinated Universal Time) or 1:30 p.m. (Mountain Time) on July 30, 2024 (the "Revocation Notice"). *See* DigiCert Notice, Compl. at Ex. 2. DigiCert asserted that the certificates needed to be revoked because they did not have a proper Domain Control Verification (DCV), which was because *DigiCert* "did not include the underscore prefix with the random value used in some CNAME-based validation cases." *Id.* In other words, *DigiCert* failed to properly validate the Alegeus Websites, and then suddenly and without any proper notice, gave Alegeus less than 21 hours to recertify each of the Alegeus Websites or face decertification.

Recertifying the Alegeus Websites requires Alegeus to coordinate with each of its Clients and cannot be completed for all of the Alegeus Websites by the DigiCert's unilaterally imposed deadline. Accordingly, Alegeus requested three days to complete recertification of the Alegeus Websites. But DigiCert has refused.

DigiCert's actions constitute a material breach of its agreement with Alegeus. Worse, if DigiCert decertifies the Alegeus Websites, it will cause Alegeus, Alegeus' Clients and each of the individual account holders severe and irreparable harm. Accordingly, Alegeus brings this action to obtain an injunction preventing DigiCert from decertifying the Alegeus Accounts and to recover for the severe damages that result from such decertification, all caused by DigiCert's actions.

FACTUAL BACKGROUND

Each of the facts set forth below has been verified by DigiCert in the Verified Complaint being filed contemporaneously herewith.

Alegeus

1. Alegeus is a leading provider of a business-to-business, white-label funding and payment platform for healthcare carriers and third-party administrators to administer consumer-directed employee benefit programs, including HSAs, FSAs, HRAs, COBRA, health and wellness programs, dependent care accounts and transportation accounts serving millions of U.S households (collectively, as defined above, the "Health Accounts").

2. In addition, Alegeus is designated as a non-bank health savings trustee ("NBT") by the IRS. This designation allows it to serve as the custodian of Health Savings Accounts ("HSAs") through a direct custodial agreement with the HSA accountholders.

3. Alegeus provides separate websites (as defined above, the "Alegeus Websites") for the Alegeus Clients.

DigiCert

4. DigiCert is a digital security company. It provides high-assurance SSL certificates to government agencies, financial institutions, educational and medical institutions, and companies worldwide.

5. DigiCert offers standard and wildcard SSL certificates, extended validation certificates, and unified communications certificates; and code signing certificate solutions that include Adobe, Apple, Java, and Microsoft code signing certificates. It also provides managed public key infrastructure solutions that allow organizations to take control of SSL certificate management, including issuing new certificates and reissuing, replacing, and revoking existing SSL certificates.

6. DigiCert is a voluntary member of the Certification Authority Browser Forum (CABF), which has bylaws stating that certificates with an issue in their domain validation must be revoked within 24 hours.

The Master Services Agreement

7. In order to obtain security certificates for the Alegeus Websites, Alegeus entered into the Master Services Agreement with DigiCert.

8. In the Master Services Agreement, DigiCert agreed to provide security certification services to Alegeus. In return, Alegeus agreed to pay for those services.

9. Specifically, the Master Services Agreement provides that:

> 2.1. Order Forms. Customer may purchase specific Services from DigiCert by entering into one or more mutually agreed upon quotes, purchase schedules, purchase orders, or order forms (whether online or electronic) that set forth the specific Services being procured by Customer under this Agreement, the term when each such Service is to be provided by DigiCert (the "Service Term") and the related payment terms for such Service (each, an "Order Form"). Order Forms are considered "mutually agreed upon" either (i) when executed by both parties in writing, (ii) when Customer affirms its electronic acceptance of an Order Form that DigiCert has presented to Customer via electronic means (e.g., at https://www.digicert.com/order), or (iii) when DigiCert presents Customer with an Order Form and Customer affirms its acceptance by issuing a purchase order. Customer and DigiCert acknowledge and agree that each Order Form will be governed by and incorporated by reference into the terms of this Agreement.

10. In June or July 2024, Alegeus ordered and paid DigiCert to update several security certificates for the Alegeus Websites.

11. Within the last 30 days, DigiCert provided updated security certificates for several of the Alegeus Websites.

DigiCert Abruptly Notices that It Intends to Revoke Alegeus' Security Certificates

12. Around 6:41 p.m. (ET) on July 29, 2024, DigiCert sent the Revocation Notice to Alegeus stating that it intended to revoke the Security Certificates for each of the Alegeus Websites.

13. The Revocation Notice stated:

> We're writing to inform you that DigiCert must revoke your certificates, no later than JULY 30, 2024, at 19:30 UTC.
>
> To avoid disruption, you must reissue/rekey and reinstall the impacted certificates before they are revoked no later than JULY 30, 2024, at 19:30 UTC.

Revocation Notice at 1.

14. The Revocation Notice explained that DigiCert's error caused the need for Alegeus to reissue/rekey and reinstall the Security Certificates for the Alegeus Websites. *Id.* Specifically, it explained:

> DigiCert will be revoking certificates that did not have proper Domain Control Verification (DCV). Before issuing a certificate to a customer, DigiCert validates the customer's control or ownership over the domain name for which they are requesting a certificate using one of several methods approved by the CA/Browser Forum (CABF). One of these methods relies on the customer adding a DNS CNAME record which includes a random value provided to them by DigiCert. DigiCert then does a DNS lookup for the domain and verifies the same random value, thereby proving domain control by the customer.
>
> There are multiple valid ways to add a DNS CNAME record with the random value provided for this purpose. One of them requires the random value to be prefixed with an underscore character. The underscore prefix ensures that the random value cannot collide with an actual domain name that uses the same random value. While the odds of that happening are practically negligible, the validation is still deemed as non-compliant if it does not include the underscore prefix.
>
> **Recently, we learned that we did not include the underscore prefix with the random value used in some CNAME-based validation cases.** This impacted approximately 0.4% of the domain validations we have in effect. Under strict CABF rules, certificates with an issue in their domain validation must be revoked within 24 hours, without exception.

Id. (emphasis added).

15. As the Revocation Notice explained, DigiCert failed to properly include the underscore prefix with the random value in certain CNAME-based validation cases. As a result, of its error, DigiCert required that Alegeus reissue/rekey and reinstall its Security Certificates. Despite it being entirely an error of DigiCert's making, DigiCert suddenly threatened that, if Alegeus failed to reissue/rekey and reinstall its Security Certificates within less than 24 hours, the Security Certificates for the Alegeus Websites would be revoked.

16. Alegeus contacted DigiCert immediately to attempt to resolve the matter within a reasonable commercial time period, including contacting its CEO. Compl. at Ex. 3. DigiCert's response is that there are no exceptions to extending the time period before revocation is to occur. *Id*.

17. On information and belief, DigiCert knew or should have known about its failure to properly complete the Security Certificates for Alegeus weeks ago. Despite that DigiCert has arbitrarily chosen this less than 24-hour window to replace defective certificates *DigiCert* provided Alegeus just a few weeks ago.

18. DigiCert's failure to properly complete the Security Certificates constitutes a material breach of the Master Services Agreement, as well as negligence and gross negligence.

Alegeus Cannot Reissue and Reinstall the Security Certificates Within 24 Hours.

19. To Reissue and Reinstall the Security Certificates, Alegeus must work and coordinate with its Clients, who are required to take steps to rectify the certificates. Alegeus has hundreds of such Clients. Alegeus is generally required by contract to give its clients much longer than 24 hours' notice before executing such a change regarding certification.

20. Consequently, due to the errors and delays of DigiCert alone, Alegeus and its Clients cannot practically make all the required changes in such a short time period and will be faced with failing to meet the terms of its Client agreements.

Revocation of the Security Certificates for the Alegeus Websites Will Cause Alegeus Severe and Irreparable Harm.

21. If DigiCert revokes the Security Certificates for the Alegeus Websites, it will cause Alegeus severe and irreparable damages.

22. Among other things, without the Security Certificates, plan participants will be unable to access and manage their accounts and a large number of participants will be unable to pay for medical services. Such a disruption (a) would impede consumers' access to healthcare accounts, (b) would subject Alegeus to high penalties for failing to meet contractual SLAs, (c) could constitute a breach of Alegeus' agreements with its clients, opening Alegeus to myriad

claims from its clients; (d) will harm Alegeus' goodwill and business reputation; and (e) cause Alegeus economic damages that cannot be readily calculated.

ARGUMENT

I. ALEGEUS HAS SATISFIED ALL REQUIREMENTS FOR INJUNCTIVE RELIEF.

The purpose of injunctive relief is to do equity. *See, e.g.*, *XMission, L.C. v. Click Sales, Inc.*, No. 2:17-CV-1287 DAK, 2019 WL 1574810, at *6 (D. Utah Apr. 11, 2019) (recognizing that the equitable nature of injunctive relief). A preliminary injunction is aimed at "prevent[ing] the perpetration of a threatened wrong" and "serves to preserve the status quo pending the outcome of the case." *Beltronics USA, Inc. V. Midwest Inventory Distribution, LLC,* 562 F.3d 1067, 1070 (10th Cir. 2009) (citing *Univ. of Texas v. Camenisch*, 451 U.S. 390, 395 (1981)). Courts have inherent authority to grant temporary restraining orders and preliminary injunctions "to preserve the status quo pending a final determination of the rights of the parties." *Resol. Tr. Corp. v. Cruce*, 972 F.2d 1195, 1198 (10th Cir. 1992) (*quoting* *Lundgrin v. Claytor*, 619 F.2d 61, 63 (10th Cir. 1980)). Granting a TRO is identical to the standard for granting a preliminary injunction. *E.g.*, *Nunez v. Nunez*, No. 1:13-CV-126-TS, 2013 WL 5230614, *2 (D. Utah 2013).

Obtaining a preliminary injunction requires demonstrating four factors: (1) a likelihood that the movant will suffer irreparable harm in the absence of preliminary relief; (2) a likelihood of success on the merits; (3) "that the balance of the equities tips in the movant's favor; and (4) that the injunction is in the public interest." *RoDa Drilling*, 552 F.3d at 1208. All four requirements are met here.

A. Alegeus Will Suffer Irreparable Harm Unless the Court Grants Preliminary Injunctive Relief.

Irreparable harm "is generally considered the most important" of the injunctive relief elements. *Greater Yellowstone Coal. v. Flowers*, 321 F.3d 1250, 1260 (10th Cir. 2003). A movant suffers irreparable harm when "the court would be unable to grant an effective monetary remedy after a full trial because such damages would be inadequate or difficult to ascertain." *Kikumura v. Hurley*, 242 F.3d 950, 963 (10th Cir. 2001). The harm need not be certain to occur. *Greater Yellowstone*, 321 F.3d at 1258. Rather, the movant need only demonstrate a "*significant risk* that he or she will experience harm that cannot be compensated after the fact by monetary damages." *Id*. Likewise, courts have routinely found irreparable harm where denying injunctive relief would result in damage to a business's reputation, goodwill, or credibility. *Dominion Video Satellite, Inc. v. Echostar Satellite Corp*., 269 F.3d 1149, 1156 (10th Cir. 2001); *Sw. Stainless, LP v. Sappington*, 581 F.3d 1176, 1191-92 (10th Cir. 2009); *XMission*, 2019 WL 1574810, at *7.

Here, with less than 21 hours' notice, DigiCert notified Alegeus of DigiCert's errors in updating the security certificates and yet threatened to revoke the Security Certificates for up to 72 of the Alegeus Websites. This will complete completely disrupt Alegeus' business operations as well as the business operations of its customers and their millions of plan participants. Indeed, depending on an individual Client security protocols, plan members will not be able to access the Alegeus Websites to manage their Health Accounts. Among other things, they will not be able to check their balances, submit reimbursements or otherwise manage the Health Accounts. This will have the practical effect of shutting down Alegeus' operations down and, even if the accounts are only declassified for a short period of time, it will destroy Alegeus' business reputation and the goodwill it has built with its clients and their plan participants.

There is no way for Alegeus to meet DigiCert's self-imposed, and unreasonably short (21-hour) recertification demand. To Reissue and Reinstall the Security Certificates, Alegeus must work with and coordinate with its Clients, who are required to take steps to rectify the certificates. Alegeus has hundreds of such Clients. Alegeus is generally required by contract to give its clients much longer than 24 hours' notice before executing such a change regarding certification. Thus, Alegeus simply cannot recertify the Security Certificates for each of the many affected Alegeus Websites in 21 hours.

As a result, if DigiCert is permitted to proceed with its revocations, Alegeus will suffer server and irreparable harm. Given the volume of certificates that will be affected, the damages will be extensive and will crush Alegeus' credibility with its clients and eviscerate its good will. There will be no way for Alegeus to adequately calculate the potential damages that will result. Accordingly, the Court should enter an order temporarily preventing DigiCert from decertifying the Security Certificates for the Alegeus Websites.

B. **There is a Substantial Likelihood Alegeus will Prevail on Its Breach of Contract Claim Against DigiCert.**

There is also a substantial likelihood that Alegeus will prevail on the merits of its claims against the DigiCert. To establish such likelihood, Plaintiff need only make a *prima facie* showing that the elements of its underlying claim can be proven. *Planned Parenthood Ass'n of Utah v. Herbert*, 828 F.3d 1245, 1252 (10th Cir. 2016). Here, as set forth in the Verified Complaint filed herewith, DigiCert's actions constitute a breach of the Master Services Agreement.

As the Court is well aware, "[t]he elements of a prima facie case for breach of contract are (1) a contract, (2) performance by the party seeking recovery, (3) breach of the contract by the other party, and (4) damages." *America West Bank Members, LC v. State*, 2014 UT 49, ¶ 15, 342 P.3d 224 (cleaned up).

The Master Services Agreement is a valid and binding contract between DigiCert and Alegeus. Compl. at Ex. 1. Pursuant to the Master Services Agreement, in June or July 2024, Alegeus engaged and paid DigiCert to update the security certificates for each of the Alegeus Websites. In return for the payment made, DigiCert was obligated to provide Alegeus with valid digital security certificates for each of the Alegeus Websites.

Despite this clear contractual obligation, and without any intervening notification, on July 29, 2024, at 4:41 p.m. (mountain), DigiCert notified Alegeus that *DigiCert* had failed to properly certify the Alegeus Websites and, as a result, Alegeus had less than 21 hours to rekey and reissue the Security Certificates for each of the Alegeus Websites or face revocation of the Security Certificates. DigiCert's actions of failing to properly provide valid digital security certificates for the Alegeus Websites constitute a breach of the Master Services Agreement. And, as set forth above, if the Security Certificates are revoked, Alegeus will suffer severe and irreparable damages. Thus, Alegeus is likely to prevail on its claim for breach of contract.

C. <u>The Threatened Injury to Alegeus Outweighs Any Harm the Injunctive Relief Could Cause DigiCert.</u>

As set forth above, revoking the certificates at issue will cause Alegeus, its clients, and the millions of plan participates that utilize Alegeus' platforms severe irreparable harm. (*See supra* A). Conversely, the requested injunctive relief permitting Alegeus seven days to resolve this issue before DigiCert is permitted to take action, will not harm DigiCert. To the contrary, this entire issue has arisen because DigiCert failed to properly certify the Alegeus Websites and then imposed a 21-hour deadline for Alegeus to fix DigiCert's error. But there is no reason why the problem needs to be resolved in 21 hours and, even if there were, this is a problem created by

DigiCert. Thus, it should bear the impact of its mistake, not Alegeus. Regardless, any harm DigiCert may face from an injunction is decidedly outweighed by the harm Alegeus and its clients and customers will experience without injunctive relief.

D. The Injunctive Relief Would Not Be Adverse to the Public Interest.

Finally, enjoining DigiCert from taking its threatened actions with respect to Alegeus' Website certificates for a short period of seven days will not be adverse to the public interest. To the contrary, granting Alegeus preliminary injunctive relief will advance the public interest.

As set forth in Alegeus' Verified Complaint, it is a financial technology provider in the healthcare space that serves as a non-bank trustee supporting millions of consumer accounts. Compl. at ¶ 15. In this capacity it manages consumer directed healthcare benefits, including flexible spending accounts (FSAs), health reimbursement accounts (HRAs) and health saving accounts (HSAs). Compl. at ¶ 14. Alegeus provides a platform that, through its health plan and administrator clients, administers healthcare benefits and provides consumers access to their healthcare related accounts. *Id.* Should DigiCert be permitted to revoke the certificates at issues, millions of plan participants and consumers will be unable to access their healthcare funds or other plan benefits until the access issues are resolved—a length of time of which Alegeus cannot estimate.

II. THE COURT SHOULD NOT REQUIRE A SECURITY.

While Rule 65 generally states that a court should require security "in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained", courts have nevertheless held that the posting of security for a preliminary injunction is vested within the court's sound discretion. *E.g.*, *Coquina Oil Corp. v. Transwestern Pipeline*, 825 F.2d 1461,1462 (10th Cir. 1987); *see also Cont'l Oil Co. v. Frontier*

Refining Co., 338 F.2d 780, 782 (10th Cir. 1964) ("trial judge has wide discretion in the matter of requiring security and if there is an absence of proof showing a likelihood of harm certainly no bond is necessary"). Here, as discussed above, DigiCert will not suffer any harm if it is precluded from revoking Alegeus' certificates for a short period of time. Thus, the security requirement should be waived.

III. ALEGEUS ATTEMPTED TO RESOLVE THE ISSSUE DIRECTLY WITH DIGICERT, BUT WAS UNSUCCESSFUL, IT WILL PROVIDE COUNSEL FOR DIGICERT WITH A COPY OF THE MOTION UPON FILING.

Since the time DigiCert provided Alegeus notice of the instant issue—yesterday at 4:41PM (Mountain)—Alegeus and its attorneys have been in ongoing contact with DigiCert and its counsel. Alegeus explained to DigiCert the necessity to filing the instant Motion if DigiCert would not delay its self-imposed deadline. Additionally, Alegeus is sending a copy of the Verified Complaint, this Motion and all related filings to DigiCert's CEO and General Counsel by email immediately upon their filing with the Court.

However, as DigiCert's 21-hour deadline will expire at 1:30 p.m. (mountain), Alegeus cannot wait for briefing and hearing. To the contrary, without an injunction by 1:30 p.m. today, Alegeus will suffer the severe and irreparable harms described above.

Alegeus was first notified of this issue at 4:41 p.m. (mountain) on July 29, 2024, and given less than 21-hours to correct an issue of DigiCert's making. While Alegeus has undertaken drastic and immediate measures in an attempt to protect its business, clients and customers, and its goodwill, its actions are incomplete, and it cannot meet the unreasonable deadline. Because injury will immediately result beginning at 1:30 p.m. (mountain), Alegeus requests that the Court immediately conduct a hearing and/or enter the proposed Temporary

Restraining Order submitted herewith. The Court can then schedule a Preliminary Injunction hearing when DigiCert and its counsel are available.

CONCLUSION

Alegeus meets each element required for preliminary injunctive relief. Thus, Alegeus respectfully requests that this Court enter a temporary restraining order precluding DigiCert from revoking Alegeus website certificates or taking any similar action with respect to Alegeus' customers, for a period of one week.

Dated this the 30th day of July 2024.

FOLEY & LARDNER LLP

/s/ *David Mortensen*
David J. Jordan
David Mortensen
Tyler A. Dever

Attorneys for Plaintiff